

UNITED STATES DISTRICT COURT

for the

Eastern District of California

FILED

Jan 12, 2021

CLERK, U.S. DISTRICT COURT  
EASTERN DISTRICT OF CALIFORNIA

In the Matter of the Search of )

A silver Apple iPhone, currently located at the )  
FBI building, located at 2001 Freedom Way in )  
Roseville, California )

Case No. 2:21-sw-00037 KJN

SEALED

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

**SEE ATTACHMENT A, attached hereto and incorporated by reference.**

located in the Eastern District of California, there is now concealed (*identify the person or describe the property to be seized*):

**SEE ATTACHMENT B, attached hereto and incorporated by reference.**

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 1591(a)(1)

Offense Description

Sex Trafficking of a Child

The application is based on these facts:

**SEE AFFIDAVIT, attached hereto and incorporated by reference.**

- ☒ Continued on the attached sheet.
- ☐ Delayed notice \_\_\_\_\_ days (give exact ending date if more than 30 \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Rachel Johnston

Applicant's signature

Rachel Johnston, FBI Special Agent

Printed name and title

Sworn to and signed telephonically pursuant to Fed. R. Crim. P. 4.1.

Date: January 12, 2021

City and state: Sacramento, California

Kendall J. Newman

Kendall J. Newman, U.S. Magistrate Judge

Printed name and title

I, Rachel Johnston, being first duly sworn, hereby depose and state as follows:

**I. INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”), and am authorized to request a search warrant pursuant to Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure. I have been an FBI Special Agent since February 2019. I joined the FBI in 2013. Prior to becoming a Special Agent, I worked as a Management and Program Analyst in the Security Division, Resource Planning Office and Counterterrorism Division. I am currently assigned to the Sacramento Division, Chico Resident Agency.

3. My law enforcement training includes twenty-one weeks of basic training at the FBI Academy in Quantico, Virginia. A portion of this training was dedicated to learning how to use computers and the Internet in order to investigate computer-related crimes. Some of my investigative responsibilities include investigation of child exploitation, national security, violent crimes, murders, bank robberies, drug trafficking and manufacturing, and firearms violations.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, law enforcement officers, and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, I submit that there is probable cause to believe: (i) that violations of 18 U.S.C. § 1591(a)(1), Sex Trafficking of a Child, have been committed by Angel Jesus Sanchez-Manriquez, and (ii) that evidence, fruits, and instrumentalities of these crimes, as described in Attachment B, will be found in the electronic device identified in Attachment A.

**II. IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

6. The property to be searched is a silver Apple iPhone (the “Subject Device”). The Subject Device is currently located at the FBI building, located at 2001 Freedom Way in Roseville, California.

7. The warrant for which I am applying would authorize a second forensic examination of the Subject Device for the purpose of identifying electronically stored data particularly described in Attachment B.

8. The Subject Device is currently in the lawful possession of the FBI. It came into the FBI’s possession as described in subsequent paragraphs and in affidavits submitted in support of previously approved search warrants, which are incorporated by reference as set forth below. Therefore, while the FBI might already have all necessary authority to re-examine the Subject Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Subject Device will comply with the Fourth Amendment and other applicable laws.

**III. FACTS ESTABLISHING PROBABLE CAUSE**

**A. Law Enforcement Seized the Subject Device and Performed an Initial Forensic Examination of It.**

9. On Saturday, December 19, 2020, law enforcement seized the Subject Device from Sanchez-Manriquez. A description of the seizure of the Subject Device is set forth in the affidavit I submitted in support of search warrant number 2:20-sw-01163-DB, which I incorporate by reference and have attached to this affidavit.

10. Search warrant number 2:20-sw-01163-DB incorporated the affidavit submitted in support of search warrant number 2:20-sw-01156-DB, which I also incorporate by reference and have attached to this affidavit.

11. On December 22, 2020, the Subject Device was booked into the evidence collection room at the FBI office located at 2001 Freedom Way in Roseville, California. The Subject Device was checked out of the evidence collection room the same day by an FBI

computer forensic examiner. The FBI computer forensic examiner completed an extraction of the available data from the Subject Device. The FBI computer forensic examiner then uploaded the results of this data extraction into an FBI computer system for my review.

**B. Sanchez-Manriquez Used Image and Video Files to Coordinate Prostitution Dates.**

12. On December 29, 2020, I reviewed the results of the initial data extraction performed on the Subject Device. In doing so, I reviewed and seized hundreds of SMS text messages and instant message conversations between Sanchez-Manriquez and yet-to-be-identified individuals.

13. Many of these yet-to-be-identified individuals requested that Sanchez-Manriquez coordinate “dates” for them with a minor female identified in this affidavit and in previous affidavits incorporated by reference as A.G., and requested that Sanchez-Manriquez provide them with photographic evidence that A.G. was the female with whom they were booking dates.<sup>1</sup> In response, Sanchez-Manriquez appears to have sent images and video files to these yet-to-be-identified individuals; in some instances, these individuals sent images of themselves to Sanchez-Manriquez in return.

14. In conducting my review of the results of the initial data extraction performed on the Subject Device, I also reviewed and seized SMS text messages and instant messages between Sanchez-Manriquez and A.G. in which they sent image and video files to one another.

**C. Obtaining Many of the Image and Video Files Contained on the Subject Device Would Require Re-Running the FBI’s Extraction Software.**

15. I reviewed a report summarizing the results of the initial data extraction performed on the Subject Device. In conducting my review of this report, I observed that although the number of image and video files extracted was reported, no image and video files were actually extracted from the Subject Device or available to view.

---

<sup>1</sup> As set forth in the affidavit I submitted in support of search warrant number 2:20-sw-01156-DB, I know that “date” is a term used in the prostitution industry to refer to an arranged encounter between a prostitute and a customer (i.e., a “john”), in which the john agrees to pay the prostitute for performing sex acts.

16. I discussed this disparity between the number of image and video files located on the Subject Device and the number of such files actually extracted from the Subject Device with the FBI computer examiner who performed the initial data extraction on the Subject Device. The FBI computer examiner informed me that because the Subject Device is a more recent iPhone model, it is likely that updating and re-running the FBI's extraction software on the Subject Device will extract more of the image and video files it contains.

17. The Subject Device is currently at the FBI building, located at 2001 Freedom Way in Roseville, California. In my training and experience, I know that the Subject Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Subject Device first came into the possession of the FBI.

#### **IV. TECHNICAL TERMS**

18. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a) Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also

include global positioning system (“GPS”) technology for determining the location of the device.

- b) Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c) Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d) GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio

a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e) PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- f) Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- g) IP Address: An Internet Protocol address (or simply “IP address”) is a unique

numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static-that is, long-term-IP addresses, while other computers have dynamic-that is, frequently changed-IP addresses.

- h) Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

19. Based on my training, experience, and research, I know that the Subject Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA, and tablet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

## **V. ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

20. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

### **A. Forensic evidence.**

21. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Subject Device was



used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Subject Device because:

- a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b) Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c) A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d) The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e) Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f) I know that when an individual uses an electronic device to manage the prostitution activity of a minor, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of

the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

**B. Nature of examination.**

22. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for would permit the examination of the Subject Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

**C. Manner of execution.**

23. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

**VI. CONCLUSION AND SEALING REQUEST**

24. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Subject Device described in Attachment A to seek the items described in Attachment B.

25. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation. Based upon my training and experience, I know that online criminals actively search for criminal affidavits and search warrants via the Internet, and

disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

/s/ Rachel Johnston

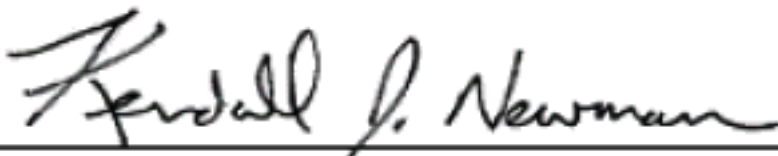
---

Rachel Johnston  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to telephonically,  
pursuant to Rule 4.1 of the Federal Rules of  
Criminal Procedure, on:

January 12, 2021

---



---

**KENDALL J. NEWMAN**  
**UNITED STATES MAGISTRATE JUDGE**

/s/ SAM STEFANKI

---

Approved as to form by:  
Assistant U.S. Attorney Sam Stefanki

**ATTACHMENT A**

The property to be searched is a silver Apple iPhone, hereinafter the “Subject Device.” The Subject Device is currently located at the FBI building, located at 2001 Freedom Way in Roseville, California.

This warrant authorizes the forensic examination of the Subject Device for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**

1. All records on the Subject Device described in Attachment A that relate to violations of 18 U.S.C. § 1591(a)(1) and involve Angel Jesus Sanchez-Manriquez, including:

- a) Records, images, audio, videos, and communications regarding A.G.;
- b) Records, images, audio, videos, and communications regarding the management of prostitution activity;
- c) Records, images, audio, videos, and communications regarding the advertisements of acts of prostitution, including use of Skipthegames.com;
- d) Records, images, audio, videos, and communications regarding hotel reservations;
- e) Records, images, audio recordings, videos, and/or communications regarding the physical location of (and transportation to and from) prostitution encounters, including stored geolocation information;
- f) Records, images, audio, video, and/or communications regarding the proceeds of prostitution activity;
- g) Information related to recruitment of individuals for the purpose of prostitution, including social media accounts that were used to engage in such recruitment;
- h) Records, images, audio, video, and communications regarding condoms, and birth control;
- i) Records, images, audio, video, and communication regarding firearms and/or ammunition;
- j) Records, images, audio, video, and communications regarding Yuba County juvenile detention facilities;
- k) Records, images, audio, video, and communications regarding ownership or control of any device assigned telephone numbers 209-420-2671 and/or 530-638-2760 and/or 916-822-9487;
- l) Records, images, audio, video, and communications regarding ownership or control of email account angelosmithx4@gmail.com and angelms99@live.com.

2. Evidence of user attribution showing who used or owned the Subject Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records evidencing the use of the following Internet Protocol addresses:

- 2601:203:c200:a3e0:751d:7159:ce43:9964;
- 2601:203:c200:a3e0:9065:9eb7:3620:b3b4;
- 2601:203:c200:a3e0:111d:70fc:a0e8:cd19;
- 2601:203:c200:a3e0:fcf3:1e26:cb1f:a702;
- 2601:203:c200:a3e0:2ddf:e21f:1c3e:55dd;

to communicate with SkiptheGames.com, including:

- a) Records of Internet Protocol addresses used;
- b) Records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

5. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Eastern District of California

FILED

Dec 21, 2020

CLERK, U.S. DISTRICT COURT  
EASTERN DISTRICT OF CALIFORNIA

In the Matter of the Search of )  
)  
silver Apple iPhone, currently located at )  
Federal Bureau of Investigation, 101 Raley )  
Boulevard, Chico, California )  
)

Case No. 2:20-sw-1163-DB

SEALED

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

**SEE ATTACHMENT A, attached hereto and incorporated by reference.**

located in the Eastern District of California, there is now concealed (*identify the person or describe the property to be seized*):

**SEE ATTACHMENT B, attached hereto and incorporated by reference**

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
18 U.S.C. § 1591(a)(1)

Offense Description  
Sex Trafficking of a Child

The application is based on these facts:

**SEE AFFIDAVIT, attached hereto and incorporated by reference.**

- ☐ Continued on the attached sheet.
- ☐ Delayed notice \_\_\_\_\_ days (give exact ending date if more than 30 \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Rachel Johnston

Applicant's signature

Rachel Johnston, FBI Special Agent

Printed name and title

Sworn to before me telephonically pursuant to Fed. R. Crim. P. 4.1.

Date: December 21, 2020



Judge's signature

City and state: Sacramento, California

Deborah Barnes, U.S. Magistrate Judge

Printed name and title

1 MCGREGOR W. SCOTT  
United States Attorney  
2 BRIAN A. FOGERTY  
Assistant United States Attorney  
3 501 I Street, Suite 10-100  
Sacramento, CA 95814  
4 Telephone: (916) 554-2700  
Facsimile: (916) 554-2900  
5

6 Attorneys for Plaintiff  
United States of America  
7

8 IN THE UNITED STATES DISTRICT COURT  
9 EASTERN DISTRICT OF CALIFORNIA  
10

11 In the Matter of the Search of:

12 silver Apple iPhone, currently located at Federal  
Bureau of Investigation, 101 Raley Boulevard,  
13 Chico, California  
14

CASE NO.

AFFIDAVIT IN SUPPORT OF AN APPLICATION  
UNDER RULE 41 FOR A WARRANT TO  
SEARCH DEVICE  
15

16 I, Rachel Johnston, being first duly sworn, hereby depose and state as follows:

17 **I. INTRODUCTION AND AGENT BACKGROUND**

18 1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of  
19 Criminal Procedure for a search warrant authorizing the examination of property—an electronic  
20 device—which is currently in law enforcement possession, and the extraction from that property of  
21 electronically stored information described in Attachment B.

22 2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”), and am  
23 authorized to request a search warrant pursuant to Rule 41(a)(2)(C) of the Federal Rules of Criminal  
24 Procedure. I have been an FBI Special Agent since February 2019. I joined the FBI in 2013. Prior to  
25 becoming a Special Agent, I worked as a Management and Program Analyst in the Security Division,  
26 Resource Planning Office and Counterterrorism Division. I am currently assigned to the Sacramento  
27 Division, Chico Resident Agency.  
28

///



1           3.       My law enforcement training includes twenty-one weeks of basic training at the FBI  
2 Academy in Quantico, Virginia. A portion of this training was dedicated to learning how to use  
3 computers and the Internet in order to investigate computer-related crimes. Some of my investigative  
4 responsibilities include investigation of child exploitation, national security, violent crimes, murders,  
5 bank robberies, drug trafficking and manufacturing, and firearms violations.

6           4.       The facts in this affidavit come from my personal observations, my training and  
7 experience, and information obtained from other agents, law enforcement officers, and witnesses. This  
8 affidavit is intended to show only that there is sufficient probable cause for the requested warrant and  
9 does not set forth all of my knowledge about this matter.

10          5.       Based on the facts set forth in this affidavit, I submit that there is probable cause (i) that  
11 violations of 18 U.S.C. § 1591(a)(1), Sex Trafficking of a Child, have been committed by Angel Jesus  
12 Sanchez-Manriquez, and (ii) that evidence, fruits, and instrumentalities of these crimes, as described in  
13 Attachment B, will be found in the electronic device identified in Attachment A.

14                   **II. IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

15          6.       The property to be searched is a silver Apple iPhone, hereinafter the “Subject Device.”  
16 The Subject Device is currently located at Federal Bureau of Investigation, 101 Raley Boulevard, Chico,  
17 California.

18          7.       The applied-for warrant would authorize the forensic examination of the Subject Device  
19 for the purpose of identifying electronically stored data particularly described in Attachment B.

20                   **III. PROBABLE CAUSE**

21          8.       I hereby incorporate the attached affidavit submitted in support of search warrant number  
22 2:20-SW-1156-DB, which authorized the search of Angel Jesus Sanchez-Manriquez.

23          9.       On Saturday, December 19, 2020, at approximately 10:13 a.m., I received a notification  
24 from AT&T regarding the location of an electronic device assigned call number 209-420-2671.<sup>1</sup> The  
25 location information<sup>2</sup> indicated that device assigned that number was north of Stockton, California, near  
26

27                   <sup>1</sup> AT&T provided the location data pursuant to search warrant number 2:20-SW-1138 DB.

28                   <sup>2</sup> The term “location information” refers to AT&T data regarding the physical location of the  
device assigned call number 209-420-2671.

1 Interstate 5. A few minutes later, at 10:29 a.m., I received additional location information that indicated  
2 that the device was located on Interstate 5, northwest of Sacramento.

3 10. The location information consistently indicated that the device was traveling north on  
4 Interstate 5 until 11:46 a.m., at which time the device entered Glenn County near the town of Willows.  
5 The location information indicated that the device was in Glenn County and around Willows between  
6 11:46 a.m. and 12:17 p.m. As set forth in the incorporated affidavit in support of search warrant number  
7 2:20-SW-1156-DB, until Friday, December 18, 2020, 16-year-old A.G. had been staying with her  
8 mother in Willows, California.

9 11. At 12:33 p.m., the location information indicated that the device was traveling south on  
10 Interstate 5. Between 12:49 p.m. and 1:20 p.m., the location information indicated that the device  
11 stopped in or around Woodland, California. At approximately 1:36 p.m., the location information  
12 indicated that the device was traveling south on Interstate 5 once again. At approximately 2:54 p.m.,  
13 location information indicated that the device was in or around 2224 East Lafayette Street, in Stockton,  
14 California (hereinafter the "2224 E. Lafayette Residence"). As set forth in the incorporated affidavit in  
15 support of search warrant number 2:20-SW-1156-DB, Sanchez-Manriquez resides at the 2224 E.  
16 Lafayette Residence.

17 12. At approximately 3:30 p.m., Stockton Police Department officers observed Sanchez-  
18 Manriquez depart the 2224 E. Lafayette Residence and drive east in an alley near the house. Sanchez-  
19 Manriquez was driving a silver Mercedes C240 with California license plate number 4RSH765.  
20 Sanchez-Manriquez turned north onto E Street, then turn left onto East Lafayette Street. Officers passed  
21 the vehicle and determined that Sanchez-Manriquez was the driver after recognizing the distinctive cross  
22 tattoo near Sanchez-Manriquez's eye. Officers turned around and stopped Sanchez-Manriquez's car  
23 directly in front of 2227 East Lafayette Street, which is across the street from the 2224 E. Lafayette  
24 Residence.

25 13. Stockton police officers approached the car from the passenger side and noticed that  
26 Sanchez-Manriquez was the only person in the car. As officers approached the car, they saw a cell  
27 phone in Sanchez-Manriquez's hand. It appeared to the officers that Sanchez-Manriquez was using this  
28 cell phone as the officers approached the car. Sanchez-Manriquez immediately told the officers that he

1 was on probation and he placed the cell phone on the front dash of the car. Officers ensured nothing  
2 was removed from the vehicle and detained Sanchez-Manriquez. Once officers searched Sanchez-  
3 Manriquez for safety purposes, handcuffed him and placed in the back of a Stockton police vehicle.

4 14. Officers went to the 2224 E. Lafayette Residence. Officers walked through the residence  
5 and asked that all of the occupants exit the residence to preserve the scene for FBI agents.

6 15. At approximately 3:32 p.m., Stockton police officers observed a white female wearing a  
7 black hooded sweatshirt and shorts walking from the alley behind the 2224 E. Lafayette Residence. The  
8 officers observed the female begin running east through the alley toward E Street. When the officers  
9 asked the female to stop, she stopped running. Officers and FBI agents later identified the female as 16-  
10 year-old A.G., who had left her mother's home the night before.

11 16. At approximately 3:53 p.m., other FBI agents and I arrived at Sanchez-Manriquez's car.  
12 I saw the Subject Device on the front dash of the car. The Subject Device was still plugged into the  
13 car's front console. FBI SA Scott Wales put the Subject Device—which Stockton police officers saw in  
14 Sanchez-Manriquez's hand during the traffic stop—into airplane mode to prevent it from receiving  
15 incoming data. SA Wales left the Subject Device plugged into the vehicle until an agent collected and  
16 photographed it at approximately 5:13 p.m. SA Wales noticed that the Subject Device's battery was low  
17 and asked that it be plugged into a power source in a Stockton police vehicle. The Subject Device  
18 stayed plugged into this vehicle until approximately 6:33 p.m. when the searches concluded. At that  
19 point, SA Wales took the Subject Device to an FBI office located at 101 Raley Boulevard in Chico,  
20 California, where it has remained in airplane mode and stored in a secure location.

21 17. The Subject Device is currently in the lawful possession of the Federal Bureau of  
22 Investigation. It came into the Federal Bureau of Investigation's possession as described in the  
23 preceding paragraphs. Therefore, while the Federal Bureau of Investigation might already have all  
24 necessary authority to examine the Subject Device, I seek this additional warrant out of an abundance of  
25 caution to be certain that an examination of the Subject Device will comply with the Fourth Amendment  
26 and other applicable laws.

27 18. The Subject Device is currently in storage at Federal Bureau of Investigation, 101 Raley  
28 Boulevard, Chico, California. In my training and experience, I know that the Device has been stored in

1 a manner in which its contents are, to the extent material to this investigation, in substantially the same  
 2 state as they were when the Subject Device first came into the possession of the Federal Bureau of  
 3 Investigation.

#### 4 **IV. TECHNICAL TERMS**

5 19. Based on my training and experience, I use the following technical terms to convey the  
 6 following meanings:

- 7 a) Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is  
 8 a handheld wireless device used for voice and data communication through radio signals.  
 9 These telephones send signals through networks of transmitter/receivers, enabling  
 10 communication with other wireless telephones or traditional “land line” telephones. A  
 11 wireless telephone usually contains a “call log,” which records the telephone number,  
 12 date, and time of calls made to and from the phone. In addition to enabling voice  
 13 communications, wireless telephones offer a broad range of capabilities. These  
 14 capabilities include: storing names and phone numbers in electronic “address books;”  
 15 sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and  
 16 storing still photographs and moving video; storing and playing back audio files; storing  
 17 dates, appointments, and other information on personal calendars; and accessing and  
 18 downloading information from the Internet. Wireless telephones may also include global  
 19 positioning system (“GPS”) technology for determining the location of the device.
- 20 b) Digital camera: A digital camera is a camera that records pictures as digital picture files,  
 21 rather than by using photographic film. Digital cameras use a variety of fixed and  
 22 removable storage media to store their recorded images. Images can usually be retrieved  
 23 by connecting the camera to a computer or by connecting the removable storage medium  
 24 to a separate reader. Removable storage media include various types of flash memory  
 25 cards or miniature hard drives. Most digital cameras also include a screen for viewing  
 26 the stored images. This storage media can contain any digital data, including data  
 27 unrelated to photographs or videos.
- 28 c) Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld

1 digital storage device designed primarily to store and play audio, video, or photographic  
2 files. However, a portable media player can also store other digital data. Some portable  
3 media players can use removable storage media. Removable storage media include  
4 various types of flash memory cards or miniature hard drives. This removable storage  
5 media can also store any digital data. Depending on the model, a portable media player  
6 may have the ability to store very large amounts of electronic data and may offer  
7 additional features such as a calendar, contact list, clock, or games.

8 d) GPS: A GPS navigation device uses the Global Positioning System to display its current  
9 location. It often contains records the locations where it has been. Some GPS navigation  
10 devices can give a user driving or walking directions to another location. These devices  
11 can contain records of the addresses or locations involved in such navigation. The Global  
12 Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites  
13 orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite  
14 repeatedly transmits by radio a mathematical representation of the current time, combined  
15 with a special sequence of numbers. These signals are sent by radio, using specifications  
16 that are publicly available. A GPS antenna on Earth can receive those signals. When a  
17 GPS antenna receives signals from at least four satellites, a computer connected to that  
18 antenna can mathematically calculate the antenna's latitude, longitude, and sometimes  
19 altitude with a high level of precision.

20 e) PDA: A personal digital assistant, or PDA, is a handheld electronic device used for  
21 storing data (such as names, addresses, appointments or notes) and utilizing computer  
22 programs. Some PDAs also function as wireless communication devices and are used to  
23 access the Internet and send and receive e-mail. PDAs usually include a memory card or  
24 other removable storage media for storing data and a keyboard and/or touch screen for  
25 entering data. Removable storage media include various types of flash memory cards or  
26 miniature hard drives. This removable storage media can store any digital data. Most  
27 PDAs run computer software, giving them many of the same capabilities as personal  
28 computers. For example, PDA users can work with word-processing documents,

1           spreadsheets, and presentations. PDAs may also include global positioning system  
2           ("GPS") technology for determining the location of the device.

3           f)     Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a  
4           notebook, that is primarily operated by touching the screen. Tablets function as wireless  
5           communication devices and can be used to access the Internet through cellular networks,  
6           802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps,  
7           which, like programs on a personal computer, perform different functions and save data  
8           associated with those functions. Apps can, for example, permit accessing the Web,  
9           sending and receiving e-mail, and participating in Internet social networks.

10          g)     IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric  
11           address used by computers on the Internet. An IP address is a series of four numbers,  
12           each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer  
13           attached to the Internet computer must be assigned an IP address so that Internet traffic  
14           sent from and directed to that computer may be directed properly from its source to its  
15           destination. Most Internet service providers control a range of IP addresses. Some  
16           computers have static-that is, long-term-IP addresses, while other computers have  
17           dynamic-that is, frequently changed-IP addresses.

18          h)     Internet: The Internet is a global network of computers and other electronic devices that  
19           communicate with each other. Due to the structure of the Internet, connections between  
20           devices on the Internet often cross state and international borders, even when the devices  
21           communicating with each other are in the same state.

22          20.     Based on my training, experience, and research, I know that the Device has capabilities  
23           that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation  
24           device, PDA, and tablet. In my training and experience, examining data stored on devices of this type  
25           can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

26                   **V.     ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

27          21.     Based on my knowledge, training, and experience, I know that electronic devices can  
28           store information for long periods of time. Similarly, things that have been viewed via the Internet are

1 typically stored for some period of time on the device. This information can sometimes be recovered  
2 with forensics tools.

3 22. Forensic evidence. As further described in Attachment B, this application seeks  
4 permission to locate not only electronically stored information that might serve as direct evidence of the  
5 crimes described on the warrant, but also forensic evidence that establishes how the Subject Device was  
6 used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic  
7 electronic evidence might be on the Subject Device because:

- 8 a) Data on the storage medium can provide evidence of a file that was once on the storage  
9 medium but has since been deleted or edited, or of a deleted portion of a file (such as a  
10 paragraph that has been deleted from a word processing file).
- 11 b) Forensic evidence on a device can also indicate who has used or controlled the device.  
12 This “user attribution” evidence is analogous to the search for “indicia of occupancy”  
13 while executing a search warrant at a residence.
- 14 c) A person with appropriate familiarity with how an electronic device works may, after  
15 examining this forensic evidence in its proper context, be able to draw conclusions about  
16 how electronic devices were used, the purpose of their use, who used them, and when.
- 17 d) The process of identifying the exact electronically stored information on a storage  
18 medium that are necessary to draw an accurate conclusion is a dynamic process.  
19 Electronic evidence is not always data that can be merely reviewed by a review team and  
20 passed along to investigators. Whether data stored on a computer is evidence may  
21 depend on other information stored on the computer and the application of knowledge  
22 about how a computer behaves. Therefore, contextual information necessary to  
23 understand other evidence also falls within the scope of the warrant.
- 24 e) Further, in finding evidence of how a device was used, the purpose of its use, who used  
25 it, and when, sometimes it is necessary to establish that a particular thing is not present on  
26 a storage medium.
- 27 f) I know that when an individual uses an electronic device to manage the prostitution  
28 activity of a minor, the individual's electronic device will generally serve both as an



instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

23. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Subject Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

24. Manner of execution. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

## **VI. CONCLUSION**

25. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Subject Device described in Attachment A to seek the items described in Attachment B.

26. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing



1 investigation and may severely jeopardize its effectiveness.

2 Respectfully submitted,

3 /s/ Rachel Johnston

4 \_\_\_\_\_  
Rachel Johnston  
5 Special Agent  
Federal Bureau of Investigation

6  
7 Subscribed and sworn to telephonically  
pursuant to Fed. R. Crim. P. 4.1 on: December 21, 2020

8 

9 \_\_\_\_\_  
10 The Honorable Deborah Barnes  
United States Magistrate Judge

11  
12  
13 /s/ Brian A. Fogerty

14 \_\_\_\_\_  
Approved as to form by:  
15 Assistant U.S. Attorney Brian A. Fogerty

**ATTACHMENT A**

The property to be searched is a silver Apple iPhone, hereinafter the “Subject Device.” The Subject Device is currently located at Federal Bureau of Investigation, 101 Raley Boulevard, Chico, California.

This warrant authorizes the forensic examination of the Subject Device for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**

1. All records on the Subject Device described in Attachment A that relate to violations of 18 U.S.C. § 1591(a)(1) and involve Angel Jesus Sanchez-Manriquez, including:
  - a. Records, images, audio, videos, and communications regarding A.G.;
  - b. Records, images, audio, videos, and communications regarding the management of prostitution activity.
  - c. Records, images, audio, videos, and communications regarding the advertisements of acts of prostitution, including use of Skipthegames.com.
  - d. Records, images, audio, videos, and communications regarding hotel reservations;
  - e. Records, images, audio recordings, videos, and/or communications regarding the physical location of (and transportation to and from) prostitution encounters, including stored geolocation information;
  - f. Records, images, audio, video, and/or communications regarding the proceeds of prostitution activity;
  - g. Information related to recruitment of individuals for the purpose of prostitution, including social media accounts that were used to engage in such recruitment;
  - h. Records, images, audio, video, and communications regarding condoms, and birth control;
  - i. Records, images, audio, video, and communication regarding firearms and/or ammunition;
  - j. Records, images, audio, video, and communications regarding Yuba County juvenile detention facilities;
  - k. Records, images, audio, video, and communications regarding ownership or control of any device assigned telephone numbers 209-420-2671 and/or 530-638-2760;
  - l. Records, images, audio, video, and communications regarding ownership or control of email account angelosmithx4@gmail.com.
2. Evidence of user attribution showing who used or owned the Subject Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
3. Records evidencing the use of the following Internet Protocol address:
  - 2601:203:c200:a3e0:751d:7159:ce43:9964;
  - 2601:203:c200:a3e0:9065:9eb7:3620:b3b4;

- 2601:203:c200:a3e0:111d:70fc:a0e8:cd19;
- 2601:203:c200:a3e0:fcf3:1e26:cb1f:a702;
- 2601:203:c200:a3e0:2ddf:e21f:1c3e:55dd;

to communicate with SkiptheGames.com, including:

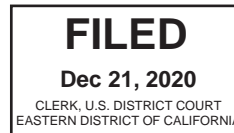
- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

4. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the  
Eastern District of California



In the Matter of the Search of  
  
Angel Jesus Sanchez-Manriquez

Case No. 2:20-sw-1156-DB

**SEALED**

**APPLICATION FOR A SEARCH WARRANT**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

**SEE ATTACHMENT A, attached hereto and incorporated by reference.**

located in the Eastern District of California, there is now concealed (*identify the person or describe the property to be seized*):

**SEE ATTACHMENT B, attached hereto and incorporated by reference**

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section*  
18 U.S.C. § 1591(a)(1)

*Offense Description*  
Sex Trafficking of a Child

The application is based on these facts:

**SEE AFFIDAVIT, attached hereto and incorporated by reference.**

- ☐ Continued on the attached sheet.
- ☐ Delayed notice        days (give exact ending date if more than 30       ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Rachel Johnston

*Applicant's signature*

Rachel Johnston, FBI Special Agent  
*Printed name and title*

Sworn to before me telephonically pursuant to Fed. R. Crim. P. 4.1.

Date: 12/19/2020

City and state: Sacramento, California

DEBORAH BARNES  
UNITED STATES MAGISTRATE JUDGE

1 MCGREGOR W. SCOTT  
United States Attorney  
2 BRIAN A. FOGERTY  
Assistant United States Attorney  
3 501 I Street, Suite 10-100  
Sacramento, CA 95814  
4 Telephone: (916) 554-2700  
Facsimile: (916) 554-2900  
5

6 Attorneys for Plaintiff  
United States of America  
7

8 IN THE UNITED STATES DISTRICT COURT  
9 EASTERN DISTRICT OF CALIFORNIA  
10

11 In the Matter of the Search of:

12 The Locations Described in Attachments A-1  
13 through A-3  
14

CASE NO.

AFFIDAVIT IN SUPPORT OF AN APPLICATION  
UNDER RULE 41 FOR WARRANTS TO SEARCH  
AND SEIZE  
15

16 I, Rachel Johnston, being first duly sworn, hereby depose and state as follows:

17 **I. INTRODUCTION AND AGENT BACKGROUND**

18 1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of  
19 Criminal Procedure for warrants to search the premises known as:

- 20 a) 2224 East Lafayette Street, Stockton, California (hereinafter, the “2224 E. Lafayette  
21 Residence”) identified in Attachment A-1 for things described in Attachment B;  
22 b) Garage building located directly behind 2226 East Lafayette Street, Stockton, California  
23 (hereinafter, the “Garage Building”) identified in Attachment A-2 for things described in  
24 Attachment B; and  
25 c) The person known as Angel Jesus Sanchez-Manriquez, further described in Attachment  
26 A-3, for the things described in Attachment B.

27 2. I am I am a Special Agent with the Federal Bureau of Investigation (“FBI”), and am  
28 authorized to request a search warrant pursuant to Rule 41(a)(2)(C) of the Federal Rules of Criminal

1 Procedure. I have been an FBI Special Agent since February 2018. I joined the FBI in 2013. Prior to  
2 becoming a Special Agent, I worked as a Management and Program Analyst in the Security Division,  
3 Resource Planning Office and Counterterrorism Division. I am currently assigned to the Sacramento  
4 Division, Chico Resident Agency.

5 3. My law enforcement training includes twenty-one weeks of basic training at the FBI  
6 Academy in Quantico, Virginia. A portion of this training was dedicated to learning how to use  
7 computers and the Internet in order to investigate computer-related crimes. Some of my investigative  
8 responsibilities include investigation of child exploitation, national security, violent crimes, murders,  
9 bank robberies, drug trafficking and manufacturing, and firearms violations.

10 4. The facts in this affidavit come from my personal observations, my training and  
11 experience, and information obtained from other agents, law enforcement officers, and witnesses. This  
12 affidavit is intended to show only that there is sufficient probable cause for the requested warrant and  
13 does not set forth all of my knowledge about this matter.

14 5. Based on the facts set forth in this affidavit, I submit that there is probable cause to  
15 believe (i) that violations of 18 U.S.C. § 1591(a)(1), Sex Trafficking of a Child, have been committed by  
16 Sanchez-Manriquez, and (ii) that evidence, fruits, and instrumentalities of these crimes, as described in  
17 Attachment B, will be found in the places identified in Attachments A-1, A-2, and A-3. Thus, the search  
18 warrant for which I am applying would authorize law enforcement agents to search the locations  
19 described in Attachments A-1 through A-3 to seize the items described in Attachment B.

20 **II. BACKGROUND REGARDING SEX TRAFFICKING**

21 6. Through my training and experience, I am aware of the following traits of prostitution as  
22 well as how the Internet and mobile telecommunications technology are used to further illegal  
23 prostitution:

- 24 a) Individuals who, through enticement, intimidation, or force, enlist other  
25 individuals to become prostitutes, and who profit from the prostitution of others,  
26 are called “pimps.”  
27 b) Pimps, as well as prostitutes, use the Internet as a means of advertising services  
28 and communicating with customers.

- 1 c) Pimps often try to recruit new victims by using social media Internet tools such as  
2 Facebook.com, Instagram, and Snapchat. Pimps often communicate with victims  
3 via social media applications after recruiting a victim to work for them.  
4 Prostitutes working for the same pimp will often use social media to communicate  
5 with each other and their pimp.
- 6 d) Certain websites facilitate communications between prostitutes and their clients.  
7 The more notable websites formerly relevant to prostitution in the Eastern District  
8 of California include the “Adult” section of Backpage.com as well as  
9 nightshift.co. New escort websites include Skipthegames.com, CityXGuide.com,  
10 Megapersonals.com, and Adultlook.com. These websites allow pictures to be  
11 posted as part of advertisements for illegal prostitution services. In the course of  
12 my career, I have viewed numerous prostitution advertisements on each of these  
13 websites and am familiar with such advertisements’ terminology, layout, and  
14 structure.
- 15 e) Pimps attempt to avoid the attention of law enforcement through the anonymity  
16 provided by the Internet.
- 17 f) Prostitutes are instructed by the pimp on how to detect undercover officers. When  
18 arranging “dates” with clients over the phone, prostitutes rarely discuss the details  
19 regarding the sexual acts that are to occur. Those more detailed discussions  
20 typically occur when the prostitute and client meet in person.
- 21 g) Pimps at times use physical force, threats of physical force, and/or fear to control  
22 prostitutes. They control the prostitutes’ actions, and collect money earned  
23 through acts of prostitution. Pimps facilitate prostitution by transporting the  
24 prostitutes to locations where the prostitution occurs. The pimps, at times,  
25 transport prostitutes across state lines for the purpose of prostitution.
- 26 h) Prostitutes and/or pimps often stay in motels and hotels while traveling.  
27 Prostitutes and pimps travel via rental vehicle, airplane, or bus during their  
28 travels. Pimps utilize the monies earned during acts of prostitution to purchase



1 food, lodging, clothing, and other items.

- 2 i) Pimps sometimes possess firearms to facilitate their sex trafficking.
- 3 j) Pimps often provide drugs to prostitutes to suppress their appetites and to help
- 4 prostitutes cope with the demands of performing sex acts for long periods of time.
- 5 k) The term “daddy” is commonly used by prostitutes when referring to their pimps.
- 6 The pimp’s phone number is often programmed as “daddy” in prostitutes’ cellular
- 7 phones.
- 8 l) Pimps often request or force their prostitutes to obtain tattoos of names and/or
- 9 symbols that are related to the pimp’s name or nickname.
- 10 m) Prostitutes use cellular telephones as a way to communicate with clients. The call
- 11 numbers associated with these cellular phones are frequently included in
- 12 advertisements posted on various websites that facilitate prostitution, including
- 13 those websites referred to earlier in this affidavit. Prostitutes, pimps, and clients
- 14 communicate via voice calls, text messages, and messages over social media
- 15 platforms.
- 16 n) Pimps and prostitutes use cellular telephones to transmit photographs to email
- 17 accounts and/or prostitution advertisement websites.
- 18 o) Pimps and prostitutes use personal email accounts to post their advertisements on
- 19 websites advertising prostitution services.

20 **III. PROBABLE CAUSE**

21 **A. A.G. Contacted a Person Using a Telephone Number Found on Online Prostitution**

22 **Advertisements That Include Photos of A.G.**

23 7. On November 12, 2020, Yuba County Sheriff’s Office Detective Natalie Mullins

24 contacted me concerning A.G.<sup>1</sup> Detective Mullins informed me that on or around November 9, 2020,

25 while in law enforcement custody at Juvenile Hall in Yuba County, A.G. asked staff at Juvenile Hall to

26 place a telephone call to her stepfather. A.G. provided Juvenile Hall staff with her purported

27

28 <sup>1</sup> A.G.’s true name and date of birth are known to law enforcement. On November 12, 2020, A.G. was sixteen years old.

stepfather's telephone number: 209-420-2671. A.G. further requested that the Juvenile Hall officer initiating the call ask for her grandfather, who she identified as "Angel."

8. The Juvenile Hall officer successfully contacted a person using the number provided by A.G. and allowed A.G. to speak to the person on the other end of the line. While A.G. was on the telephone, the Juvenile Hall officer overheard A.G. refer to the person on the other end of the line as "baby" or "babe." The officer terminated the phone call.

9. The Juvenile Hall officer conducted a Google search of the number. This search revealed that 209-420-2671 was listed as the contact telephone number on multiple online advertisements for prostitution services, some of which contained a photograph of A.G.

**B. A.G.'s Photograph Appears on Dozens of Online Posts Advertising Prostitution Services**

10. On November 13, 2020, I searched for and viewed advertisements on Skipthegames.com, in a section of the website titled "California," subsection "Stockton," subsection "Female Escort." I located over seventy separate and distinct advertisements bearing titles such as, "Snow Bunny in Stockton."

11. Each such advertisement for "Snow Bunny in Stockton" contained a photograph depicting a white female in her underwear, as well as a photograph of A.G. Many of the advertisements included a photograph of A.G. that she took of herself (i.e., a "selfie") in a light pink, off-the-shoulder top, with her hair pulled back. In this photograph, a large tattoo depicting a flower, a locket, and the word "kilo" was visible on A.G.'s right chest. Of the over seventy advertisements that I viewed on November 13, 2020 all but two included contact call number 209-420-2671.<sup>2</sup> Each advertisement listed A.G.'s age as nineteen years old. The text of each advertisement varied based on whether A.G. was

---

<sup>2</sup> One advertisement of A.G. posted to SkiptheGames.com on October 8, 2020, listed the contact telephone number as 916-822-9487. Based on subscriber information provided by Pinger, telephone number 916-822-9487 is a voice over Internet protocol (VOIP) created to communicate on the cell phone application TextFree. According to Pinger, the username for the subscriber of telephone number 916-822-9487 is Amanriquez29320. This VOIP telephone number was active between September 20, 2020 and November 10, 2020. One advertisement of A.G. posted to SkiptheGames.com on October 14, 2020, listed the contact telephone number as 209-639-9025. Based on evidence gathered during this investigation, I know that A.G.'s cellular telephone is assigned the call number 209-639-9025. When I searched A.G.'s cellular telephone pursuant to a federal search warrant, I discovered no evidence of that the device accessing SkiptheGames.com.

available for an in-call, out-call, or car date.<sup>3</sup> Some advertisement did not list her availability at all. Some advertisements included a list of things A.G. was not willing to do. At the bottom of an advertisement posted on October 8, 2020 the following is listed; “NO BB NO BBBJ NO GFE NO GREEK D.” Although the advertisements varied, each included the following content:

Hey my name is Alexis and I am located in Stockton 😊 let me please you in any way I could 📞 call or Text (phone number) for more info.

12. Based on my training and experience, I know that “BB” means “bareback” or to engage in sex without a condom; “BBBJ” means to perform oral sex without a condom; and “Greek” means to have anal sex.

13. On November 17, 2020, I interviewed A.G. at Juvenile Hall. I showed A.G. a copy of the “selfie” described above, and A.G confirmed that she is the person depicted in that photograph. During this interview, A.G. also confirmed that she had recently turned sixteen years old.

**C. 209-420-2671 Belongs to Sanchez-Manriquez.**

14. I performed searches of various public and employment records. These searches revealed to me that the call number 209-420-2671 belongs to Sanchez-Manriquez and is associated with an AT&T cellular telephone account. According to AT&T records, an individual named Yesenia Manriquez paid the bill for this account between March 2020 and October 2020. AT&T records also indicate that Yesenia Manriquez is also a “top contact” for the account associated with 209-420-2671. According to Stockton Police Department probation information, Sanchez-Manriquez’s mother is Yesenia Manriquez.

15. I interviewed A.G.'s mother on December 1, 2020. A.G.'s mother told me that on or about November 8, 2020, A.G.'s mother began communicating with a person she knew as Angel via text message. A.G.'s mother reported that Angel was using a phone assigned the call number 209-420-2671 to send and receive text messages with A.G.'s mother. Angel identified himself to A.G.'s mother and informed A.G.'s mother that he wanted to give A.G.'s mother \$2,000 in cash that he claimed belonged

<sup>3</sup> Based on my training and experience, I know that an “in-date” is when a prostitution customer travels to the sex worker for the encounter; and “out-call” is when the sex worker travels to the prostitution customer to perform the sexual encounter; and a “car date” is when the sexual encounter occurs in a vehicle.

1 to A.G., as well as some of A.G.'s personal belongings.<sup>4</sup>

2 16. A.G.'s mother further informed me that after A.G. contacted Angel from Juvenile Hall,  
3 on or around November 12, 2020 the tone of Angel's text messages to A.G.'s mother changed.

4 17. On November 9, 2020, a person using telephone number 530-638-2760 sent a text to  
5 A.G.'s mother, in which the person identified himself or herself as "Jen," a neighbor. Jen told A.G.'s  
6 mother that a Hispanic kid asked to use her phone because he had A.G.'s belongings and wanted to give  
7 them to her. A.G.'s mother did not respond. On November 19, 2020, a person using telephone number  
8 530-638-2760 sent A.G.'s mother a short video that depicted two people in the front seat of a car holding  
9 Glock-style firearms. The following text message exchange took place after the video was sent:

10 530-638-2760: Come out [A.G.'s mother's first name] I have a message,  
11 I'm outside [name of apartment building] ☺

12 A.G.'s mother: Lol I'm outside. U don't scare me with gun threats. Are u  
threatening my life?

13 530-638-2760: Come walk to the alley behind McDonald's. I never  
14 enforced a thread

15 A.G.'s mother: What u gonna murder me over me not wanting my  
Daughter to get screwed over?

16 530-638-2760: I heard your interfering with business I wa so my sent to  
17 give u a message

18 A.G.'s mother: Who is this even?

19 530-638-2760: My nephew is to not be fucked with. Small fries like u get  
20 plucked for less. My nephew said you daughter is lowing and u continue  
to bug him

21 A.G.'s mother: I'm not fucking With no one he just has \$2,000 of  
daughter's money that's all.

22 530-638-2760: Your daughter doesn't have money

23 A.G.'s mother: I just asked for her clothes and her money she worked for  
24 that's it. I don't want no problems but I will stand up for Baby girl.

25 530-638-2760: Is your life worth listening to your daughters lies? Yes or  
No. I don't want no answer besides yes or no.

26 A.G.'s mother: Look I known what ur about I'm just making sure my  
27

28 <sup>4</sup> A.G.'s mother also informed me that in the course of her text message exchange with Angel in  
early November 2020, Angel told her that A.G. had been residing with Angel for around two months.

1 daughter don't get screwed over that's it.

2 530-638-2760: Your daughter has nothing with us. Your daughter used us  
3 and u continue to escalate these problems. Now tell me.

4 A.G.'s mother: I asked him nicely he was the one that was threatening my  
5 life over some shit I'm not scared of a gun

6 530-638-2760: Is your life worth losing over your daughter lies? Yes or  
7 no. Tell me

8 18. Based on subscriber information provided by Pinger, telephone number 530-638-2760 is  
9 a VOIP number created to communicate on the cell phone application TextFree. According to Pinger,  
10 the name of the account is "Angel" and the username is "Angelsm99." This VOIP telephone number  
11 was created on November 9, 2020 and is still active as of December 4, 2020.

12 **D. Additional Facts Connecting A.G. to Sanchez-Manriquez and Prostitution.**

13 19. In or around November 2020, Detective Mullins gave me three photographs of A.G. that  
14 I had not previously seen. Two of these photographs include a Hispanic male. I believe Sanchez-  
15 Manriquez is the Hispanic male depicted in the photographs that Detective Mullins gave me because I  
16 compared his California driver's license photograph to the person depicted in the photographs with A.G.  
17 Based on the similar physical appearance of the individuals depicted in the photos, I concluded that the  
18 two photos depicting a Hispanic male actually depict the same person: Sanchez-Manriquez.

19 20. On December 8, 2020, the Honorable Allison Claire issued search warrant number 2:20-  
20 sw-01115-AC, which authorized the search of the Apple iPhone cell phone A.G. possessed at Juvenile  
21 Hall. Pursuant to that search warrant, I conducted a search of A.G.'s iPhone, which was activated on or  
22 around October 13, 2020. During my review of A.G.'s iPhone, I found multiple images of A.G. and  
23 Sanchez-Manriquez posing together in bed. In at least one of these photographs, A.G. is partially nude.

24 **Text Messages From A.G.'s iPhone.**

25 21. While searching A.G.'s iPhone, I viewed a text message exchange between A.G. and a  
26 so-far-unidentified prostitution customer that occurred on November 7, 2020. In summary, A.G. and  
27 this unidentified prostitution customer attempted to schedule a "date"—or prostitution encounter—for  
28 November 8, 2020, between 9:30 a.m. and 10:00 a.m. The date texted "would you do it for \$100?"  
A.G. responded "yes." A.G. told the prostitution customer that the date would take place in room 227 at

1 the Motel 6 located at 6717 Plymouth Road in Stockton, California.

2 22. At 10:02 a.m. on November 8, 2020, A.G. and Sanchez-Manriquez, who was saved in  
3 A.G.'s device under telephone number 209-420-2671 as "Angel," engaged in the following iMessage  
4 exchange:

5 Sanchez-Manriquez: Ima have my black homies in room 225 go get u.  
6 They been watching u. If u don't answer.

7 A.G.: Nigga I have a trick rn. He's coming.<sup>5</sup>

8 Sanchez-Manriquez: I have one going too

9 A.G.: And tbh I would have paid but I put them in the toilet.

10 Sanchez-Manriquez: I'm calling hotel security to kick u out

11 A.G.: And okay. For what I didn't do shit.

12 23. During my review of A.G.'s phone, I also found Google searches for hotels in Stockton  
13 California, and screenshots of hotels in that area. On October 13, 2020 and October 14, 2020, A.G.'s  
14 phone was connected to the WiFi at a Days Inn. On November 2, A.G.'s cell phone was connected to  
15 the WiFi at a Rodeway Inn. On November 7, 2020, A.G.'s cell phone was connected to WiFi named  
16 "Yesenia," which is Sanchez-Manriquez's mother's first name.

17 24. On an unknown date and time, A.G. engaged in a text message conversation with a  
18 contact saved in her iPhone as "Chupo." This exchange proceeded as follows:

19 Chupo: I kno u probably like what u do but honestly u a pretty as girl and u  
20 don't have to do wat ur doing. U can get a job a be koo. Its not like ur  
21 doing it for u so think about that go home be good get a boyfriend that  
22 loves u and don't just want to take yo cheese. U hella koo and u should be  
23 happy. Stop doing them pills homie bad for u.

24 A.G.: I don't really like what I'm doing I only do this cuz angel started  
25 into getting me to do this I've never done it for money and shit and thank  
26 u but u got what u wanted me and him aint together so I hope u happy.  
27 Take care of him. And I right. U\*

28 <sup>5</sup> Based on my training and experience, I know that that in the prostitution industry, the term  
"trick" refers to a prostitution customer.

Subscriber Information Connecting Sanchez-Manriquez's Prostitution Operation  
to Sanchez-Manriquez's Residence.

25. On November 16, 2020, a representative of SkiptheGames.com provided subscriber information (including Internet Protocol ("IP") addresses) for the user who posted prostitution advertisements containing A.G.'s photograph. According to these records, the user who posted these advertisements logged into Skipthegames.com from an account associated with the call number 209-420-2671 and associated with the email address angelosmithx4@gmail.com.<sup>6</sup>

26. Comcast records indicate that five of the IP addresses from which advertisements of A.G. were posted to SkiptheGames.com were assigned by Comcast to Yesenia Manriquez as follows:

- a) 2601:203:c200:a3e0:751d:7159:ce43:9964 (assigned on November 4, 2020);
- b) 2601:203:c200:a3e0:9065:9eb7:3620:b3b4 (assigned on November 4, 2020);
- c) 2601:203:c200:a3e0:111d:70fc:a0e8:cd19 (assigned on November 4, 2020);
- d) 2601:203:c200:a3e0:fcf3:1e26:cb1f:a702 (assigned on November 6, 2020); and
- e) 2601:203:c200:a3e0:2ddf:e21f:1c3e:55dd (assigned on November 6, 2020).

27. The address of service provided by Comcast for these five IP addresses on these dates was 2224 East Lafayette Street, Stockton, California (i.e., the 2224 E. Lafayette Residence).

28. Based on searches of open-source data, I determined that AT&T Mobility provided all the remaining IP addresses from which advertisements of A.G. were posted to SkiptheGames.com. Based on my training and experience, I know this to mean that these remaining IP addresses were used by an AT&T subscriber to access the Internet from a mobile device such as a cellular telephone. AT&T does not maintain records connecting mobile IP addresses of this type to particular devices or accounts. As set forth above, the AT&T account associated with call number 209-420-2671 is paid for by Yesenia Manriquez.

///

///

---

<sup>6</sup> I believe that the Google email address [angelosmithx4@gmail.com](mailto:angelosmithx4@gmail.com) is at times being used by an individual named Angelo Smith. On September 27, 2020, officers from the Stockton Police Department conducted a traffic stop of a vehicle in which Sanchez-Manriquez and Smith were both passengers.



Sanchez-Manriquez lives at 2224 E. Lafayette Residence.

29. Sanchez-Manriquez is currently on probation ordered by a San Joaquin County Superior Court Judge. According to records provided to me by the Stockton Police Department, Sanchez-Manriquez's residence address for purposes of his probation is the 2224 E. Lafayette Residence.

30. According to records maintained by the California Department of Motor Vehicles, the 2224 E. Lafayette Residence is Sanchez-Manriquez's address on his California driver's license, which was last updated on January 28, 2020.

31. On December 16, 2020, officers from the Stockton Police Department conducted surveillance of the 2224 E. Lafayette Residence. During surveillance, officers observed Sanchez-Manriquez in the Garage Building that abuts the 2224 E. Lafayette Residence. The Garage Building is shared by 2224 and 2226 E. Lafayette Street. Sanchez-Manriquez's maternal grandparents reside at 2226 E. Lafayette Street.

**E. A.G.'s Mother Recently Reported Her Missing.**

32. On December 19, 2020, A.G.'s mother informed me that A.G. left her home on the evening of December 18, 2020. A.G.'s mother reported that she has not had contact with A.G. and does not know where A.G. went.

33. On December 14, 2020, this Court authorized the collection of precise location data concerning Sanchez-Manriquez's cell phone that is assigned telephone number 209-420-2671. AT&T has provided location data for that cell phone, which indicates that on the morning of December 19, 2020, the device traveled from the vicinity of Stockton, California—the location of the 2224 E. Lafayette Residence and Garage Building—to Willows, California. A.G.'s mother resides in Willows, California. The location data also indicates that the device stayed in Willows for approximately 30 minutes, then began traveling south on Interstate 5 in the direction of Stockton, California.

**IV. TECHNICAL TERMS**

34. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a) IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. Typically, an IP address looks like a series of



four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Other forms of IP addresses, such as IPv6, may express IP addresses differently. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b) Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c) Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

## **V. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

35. As described above and in Attachment B, this application seeks permission to search for records that might be found in the places identified in Attachments A-1 through A-3, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

36. *Probable cause.* I submit that if a computer or storage medium is found in the place identified in Attachments A-1 through A-3, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools.

1 This is so because when a person “deletes” a file on a computer, the data contained in the  
 2 file does not actually disappear; rather, that data remains on the storage medium until it is  
 3 overwritten by new data.

4 b) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack  
 5 space—that is, in space on the storage medium that is not currently being used by an  
 6 active file—for long periods of time before they are overwritten. In addition, a  
 7 computer’s operating system may also keep a record of deleted data in a “swap” or  
 8 “recovery” file.

9 c) Wholly apart from user-generated files, computer storage media—in particular,  
 10 computers’ internal hard drives—contain electronic evidence of how a computer has been  
 11 used, what it has been used for, and who has used it. To give a few examples, this  
 12 forensic evidence can take the form of operating system configurations, artifacts from  
 13 operating system or application operation, file system data structures, and virtual memory  
 14 “swap” or paging files. Computer users typically do not erase or delete this evidence,  
 15 because special software is typically required for that task. However, it is technically  
 16 possible to delete this information.

17 d) Similarly, files that have been viewed via the Internet are sometimes automatically  
 18 downloaded into a temporary Internet directory or “cache.”

19 37. *Forensic evidence.* As further described in Attachment B, this application seeks  
 20 permission to locate not only computer files that might serve as direct evidence of the crimes described  
 21 on the warrant, but also for forensic electronic evidence that establishes how computers were used, the  
 22 purpose of their use, who used them, and when. There is probable cause to believe that this forensic  
 23 electronic evidence will be on any storage medium in the location identified in the Attachments because:

24 a) Data on the storage medium can provide evidence of a file that was once on the storage  
 25 medium but has since been deleted or edited, or of a deleted portion of a file (such as a  
 26 paragraph that has been deleted from a word processing file). Virtual memory paging  
 27 systems can leave traces of information on the storage medium that show what tasks and  
 28 processes were recently active. Web browsers, e-mail programs, and chat programs store

1 configuration information on the storage medium that can reveal information such as  
2 online nicknames and passwords. Operating systems can record additional information,  
3 such as the attachment of peripherals, the attachment of USB flash storage devices or  
4 other external storage media, and the times the computer was in use. Computer file  
5 systems can record information about the dates files were created and the sequence in  
6 which they were created, although this information can later be falsified.

7 b) As explained herein, information stored within a computer and other electronic storage  
8 media may provide crucial evidence of the “who, what, why, when, where, and how” of  
9 the criminal conduct under investigation, thus enabling the United States to establish and  
10 prove each element or alternatively, to exclude the innocent from further suspicion. In  
11 my training and experience, information stored within a computer or storage media (e.g.,  
12 registry information, communications, images and movies, transactional information,  
13 records of session times and durations, internet history, and anti-virus, spyware, and  
14 malware detection programs) can indicate who has used or controlled the computer or  
15 storage media. This “user attribution” evidence is analogous to the search for “indicia of  
16 occupancy” while executing a search warrant at a residence. The existence or absence of  
17 anti-virus, spyware, and malware detection programs may indicate whether the computer  
18 was remotely accessed, thus inculcating or exculpating the computer owner. Further,  
19 computer and storage media activity can indicate how and when the computer or storage  
20 media was accessed or used. For example, as described herein, computers typically  
21 contains information that log: computer user account session times and durations,  
22 computer activity associated with user accounts, electronic storage media that connected  
23 with the computer, and the IP addresses through which the computer accessed networks  
24 and the internet. Such information allows investigators to understand the chronological  
25 context of computer or electronic storage media access, use, and events relating to the  
26 crime under investigation. Additionally, some information stored within a computer or  
27 electronic storage media may provide crucial evidence relating to the physical location of  
28 other evidence and the suspect. For example, images stored on a computer may both

1 show a particular location and have geolocation information incorporated into its file  
2 data. Such file data typically also contains information indicating when the file or image  
3 was created. The existence of such image files, along with external device connection  
4 logs, may also indicate the presence of additional electronic storage media (e.g., a digital  
5 camera or cellular phone with an incorporated camera). The geographic and timeline  
6 information described herein may either inculcate or exculpate the computer user. Last,  
7 information stored within a computer may provide relevant insight into the computer  
8 user's state of mind as it relates to the offense under investigation. For example,  
9 information within the computer may indicate the owner's motive and intent to commit a  
10 crime (e.g., internet searches indicating criminal planning), or consciousness of guilt  
11 (e.g., running a "wiping" program to destroy evidence on the computer or password  
12 protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- 13 c) A person with appropriate familiarity with how a computer works can, after examining  
14 this forensic evidence in its proper context, draw conclusions about how computers were  
15 used, the purpose of their use, who used them, and when.
- 16 d) The process of identifying the exact files, blocks, registry entries, logs, or other forms of  
17 forensic evidence on a storage medium that are necessary to draw an accurate conclusion  
18 is a dynamic process. While it is possible to specify in advance the records to be sought,  
19 computer evidence is not always data that can be merely reviewed by a review team and  
20 passed along to investigators. Whether data stored on a computer is evidence may  
21 depend on other information stored on the computer and the application of knowledge  
22 about how a computer behaves. Therefore, contextual information necessary to  
23 understand other evidence also falls within the scope of the warrant.
- 24 e) Further, in finding evidence of how a computer was used, the purpose of its use, who  
25 used it, and when, sometimes it is necessary to establish that a particular thing is not  
26 present on a storage medium. For example, the presence or absence of counter-forensic  
27 programs or anti-virus programs (and associated data) may be relevant to establishing the  
28 user's intent.

1 f) I know that when an individual uses a computer to manage the prostitution activity of a  
2 minor, the individual's computer will generally serve both as an instrumentality for  
3 committing the crime, and also as a storage medium for evidence of the crime. The  
4 computer is an instrumentality of the crime because it is used as a means of committing  
5 the criminal offense. The computer is also likely to be a storage medium for evidence of  
6 crime. From my training and experience, I believe that a computer used to commit a  
7 crime of this type may contain: data that is evidence of how the computer was used; data  
8 that was sent or received; notes as to how the criminal conduct was achieved; records of  
9 Internet discussions about the crime; and other records that indicate the nature of the  
10 offense.

11 38. *Necessity of seizing or copying entire computers or storage media.* In most cases, a  
12 thorough search of a premises for information that might be stored on storage media often requires the  
13 seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of  
14 removing storage media from the premises, it is sometimes possible to make an image copy of storage  
15 media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's  
16 data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to  
17 ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of  
18 the data either from accidental or intentional destruction. This is true because of the following:

- 19 a) The time required for an examination. As noted above, not all evidence takes the form of  
20 documents and files that can be easily viewed on site. Analyzing evidence of how a  
21 computer has been used, what it has been used for, and who has used it requires  
22 considerable time, and taking that much time on premises could be unreasonable. As  
23 explained above, because the warrant calls for forensic electronic evidence, it is  
24 exceedingly likely that it will be necessary to thoroughly examine storage media to obtain  
25 evidence. Storage media can store a large volume of information. Reviewing that  
26 information for things described in the warrant can take weeks or months, depending on  
27 the volume of data stored, and would be impractical and invasive to attempt on-site.
- 28 b) Technical requirements. Computers can be configured in several different ways,

featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c) Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

39. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

40. Because several people share the 2224 E. Lafayette Residence and Garage Building as a residence, it is possible that these premises will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

## VI. CONCLUSION

41. I submit that this affidavit supports probable cause for a warrant to search the locations described in Attachments A-1 through A-3 and seize the items described in Attachment B.

## VII. REQUEST FOR SEALING

42. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I

1 believe that sealing this document is necessary because the items and information to be seized are  
2 relevant to an ongoing investigation into the criminal organizations as not all of the targets of this  
3 investigation will be searched at this time. Based upon my training and experience, I have learned that  
4 online criminals actively search for criminal affidavits and search warrants via the Internet, and  
5 disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online  
6 through the carding forums. Premature disclosure of the contents of this affidavit and related documents  
7 may have a significant and negative impact on the continuing investigation and may severely jeopardize  
8 its effectiveness.

10 Respectfully submitted,

11 /s/ Rachel Johnston

12 Rachel Johnston  
13 Special Agent  
14 Federal Bureau of Investigation

15 Subscribed and sworn telephonically  
16 on:

12/19/2020

17   
18 \_\_\_\_\_  
19 DEBORAH BARNES  
20 UNITED STATES MAGISTRATE JUDGE

21 /s/ Brian A. Fogerty

22 Approved as to form by:  
23 Assistant U.S. Attorney Brian A. Fogerty



**ATTACHMENT A-1**

The property to be searched is 2224 East Lafayette Street, Stockton, California (i.e., the “2224 E. Lafayette Residence”), including the residential building, any outbuildings, and any appurtenances thereto, any cell phone, computer or storage medium found therein, and any person located at the property. The property is a brown stucco house with a white front door, as depicted below:





**ATTACHMENT A-2**

The property to be searched is a garage building that abuts the residence at 2226 East Lafayette Street, Stockton, California (i.e., the “Garage Building”), including the residential building, any outbuildings, and any appurtenances thereto, any cell phone, computer or storage medium found therein, and any person located at the property. The property is depicted below:



**ATTACHMENT A-3**

The person to be searched is Angel Jesus Sanchez-Manriquez, date of birth April 7, 1999, including any containers, cell phones, computers or storage medium found thereon. Set forth below is a photo of Angel Jesus Sanchez-Manriquez:



**ATTACHMENT B**

**Items to be seized**

1. All records relating to violations of 18 U.S.C. §§ 1591(a)(1), Sex Trafficking of a Child, those violations involving Angel Jesus Sanchez-Manriquez, including:

- a. Records, images, audio, videos, and communications regarding A.G.;
- b. Records, images, audio, videos, and communications regarding the management of prostitution activity.
- c. Records, images, videos, and communications regarding the advertisements of acts of prostitution, including use of Skipthegames.com.
- d. Records, images, videos, and communications regarding hotel reservations;
- e. Hotel room keys;
- f. Records, images, audio recordings, videos, and/or communications regarding the physical location of (and transportation to and from) prostitution encounters, including stored geolocation information;
- g. Information related to recruitment or potential recruitment of individuals for the purpose of prostitution, including social media accounts that may have been used to engage in such recruitment;
- h. Condoms;
- i. Sex toys;
- j. Any cell phone, computer, or electronic storage media currently or previously assigned call number 209- 420-2671 and/or 530-638-2760;
- k. Firearms and/or ammunition;
- l. U.S. mail addressed to A.G.;
- m. Clothing, identification, and/or electronic devices that belonged to individuals who engaged in prostitution.

n. Records, images, videos, and communications regarding any travel involving A.G. for the purpose of engaging in prostitution;

s. United States currency that is the proceeds of prostitution;

t. Indicia of occupancy, residency, control or ownership of the premises and the things described in this warrant, including utility bills, telephone bills, loan repayment receipts, rent documents, envelopes and keys, photographs, and bank records;

2. Computers or storage media used as a means to commit the violations described above, including computers or storage media used to manage prostitution.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

5. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a

complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the  
Eastern District of California

In the Matter of the Search of  
  
Angel Jesus Sanchez-Manriquez

Case No. 2:20-sw-1156-DB

**SEALED**

**SEARCH AND SEIZURE WARRANT**

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the \_\_\_\_\_ Eastern \_\_\_\_\_ District of \_\_\_\_\_ California \_\_\_\_\_  
(identify the person or describe the property to be searched and give its location):

**SEE ATTACHMENT A, attached hereto and incorporated by reference.**

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

**SEE ATTACHMENT B, attached hereto and incorporated by reference.**

**YOU ARE COMMANDED** to execute this warrant on or before \_\_\_\_\_ January 2, 2021 \_\_\_\_\_ (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to: any authorized U.S. Magistrate Judge in the Eastern District of California.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for \_\_\_\_\_ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_ .

Date and time issued: \_\_\_\_\_ 12/19/2020, 3:30pm \_\_\_\_\_

City and state: \_\_\_\_\_ Sacramento, California \_\_\_\_\_

  
DEBORAH BARNES  
UNITED STATES MAGISTRATE JUDGE

**Return**

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

\_\_\_\_\_  
Subscribed, sworn to, and returned before me this date.

\_\_\_\_\_  
Signature of Judge

\_\_\_\_\_  
Date



UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of

silver Apple iPhone, currently located at Federal  
Bureau of Investigation, 101 Raley Boulevard, Chico,  
California

Case No. 2:20-sw-1163-DB

**SEALED**

**SEARCH AND SEIZURE WARRANT**

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the \_\_\_\_\_ Eastern \_\_\_\_\_ District of \_\_\_\_\_ California  
(identify the person or describe the property to be searched and give its location):

**SEE ATTACHMENT A, attached hereto and incorporated by reference.**

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

**SEE ATTACHMENT B, attached hereto and incorporated by reference.**

**YOU ARE COMMANDED** to execute this warrant on or before \_\_\_\_\_ January 4, 2021 \_\_\_\_\_ (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to: any authorized U.S. Magistrate Judge in the Eastern District of California.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for \_\_\_\_\_ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_.

Date and time issued: December 21, 2020 at 3:51 p.m.



Judge's signature

City and state: Sacramento, California

Deborah Barnes, U.S. Magistrate Judge

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2) (modified)

<b>Return</b>		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		
<b>Certification</b>		
<p>I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.</p>  <div style="text-align: center;"> <hr style="width: 80%; margin: 0 auto;"/> <p>Subscribed, sworn to, and returned before me this date.</p> </div>  <div style="display: flex; justify-content: space-between; margin-top: 20px;"> <div style="width: 60%;"> <hr style="width: 80%; margin: 0 auto;"/> <p style="text-align: center; margin-top: 5px;">Signature of Judge</p> </div> <div style="width: 35%; text-align: center;"> <hr style="width: 80%; margin: 0 auto;"/> <p style="text-align: center; margin-top: 5px;">Date</p> </div> </div>		

**ATTACHMENT A**

The property to be searched is a silver Apple iPhone, hereinafter the “Subject Device.” The Subject Device is currently located at Federal Bureau of Investigation, 101 Raley Boulevard, Chico, California.

This warrant authorizes the forensic examination of the Subject Device for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**

1. All records on the Subject Device described in Attachment A that relate to violations of 18 U.S.C. § 1591(a)(1) and involve Angel Jesus Sanchez-Manriquez, including:
  - a. Records, images, audio, videos, and communications regarding A.G.;
  - b. Records, images, audio, videos, and communications regarding the management of prostitution activity.
  - c. Records, images, audio, videos, and communications regarding the advertisements of acts of prostitution, including use of Skipthegames.com.
  - d. Records, images, audio, videos, and communications regarding hotel reservations;
  - e. Records, images, audio recordings, videos, and/or communications regarding the physical location of (and transportation to and from) prostitution encounters, including stored geolocation information;
  - f. Records, images, audio, video, and/or communications regarding the proceeds of prostitution activity;
  - g. Information related to recruitment of individuals for the purpose of prostitution, including social media accounts that were used to engage in such recruitment;
  - h. Records, images, audio, video, and communications regarding condoms, and birth control;
  - i. Records, images, audio, video, and communication regarding firearms and/or ammunition;
  - j. Records, images, audio, video, and communications regarding Yuba County juvenile detention facilities;
  - k. Records, images, audio, video, and communications regarding ownership or control of any device assigned telephone numbers 209-420-2671 and/or 530-638-2760;
  - l. Records, images, audio, video, and communications regarding ownership or control of email account angelosmithx4@gmail.com.
2. Evidence of user attribution showing who used or owned the Subject Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
3. Records evidencing the use of the following Internet Protocol address:
  - 2601:203:c200:a3e0:751d:7159:ce43:9964;
  - 2601:203:c200:a3e0:9065:9eb7:3620:b3b4;

- 2601:203:c200:a3e0:111d:70fc:a0e8:cd19;
- 2601:203:c200:a3e0:fcf3:1e26:cb1f:a702;
- 2601:203:c200:a3e0:2ddf:e21f:1c3e:55dd;

to communicate with SkiptheGames.com, including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

4. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

## UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of )

A silver Apple iPhone, currently located at the FBI  
 building, located at 2001 Freedom Way in Roseville,  
 California )

Case No. 2:21-sw-0037 KJN

**SEALED****SEARCH AND SEIZURE WARRANT**

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search  
 of the following person or property located in the \_\_\_\_\_ Eastern \_\_\_\_\_ District of \_\_\_\_\_ California  
*(identify the person or describe the property to be searched and give its location):*

**SEE ATTACHMENT A, attached hereto and incorporated by reference.**

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
 described above, and that such search will reveal *(identify the person or describe the property to be seized):*

**SEE ATTACHMENT B, attached hereto and incorporated by reference.****YOU ARE COMMANDED** to execute this warrant on or before \_\_\_\_\_ January 26, 2021 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

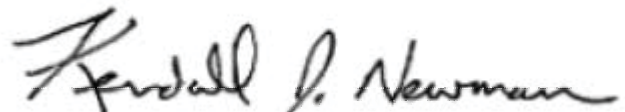
Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
 person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
 property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
 as required by law and promptly return this warrant and inventory to: any authorized U.S. Magistrate Judge in the Eastern  
 District of California.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
 § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
 property, will be searched or seized *(check the appropriate box)*

☐ for \_\_\_\_\_ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of \_\_\_\_\_.

Date and time issued: \_\_\_\_\_  
 January 12, 2021 at 11:40 a.m.



City and state: \_\_\_\_\_  
 Sacramento, California

Kendall J. Newman, U.S. Magistrate Judge

*Printed name and title*

[illegible]

**ATTACHMENT A**

The property to be searched is a silver Apple iPhone, hereinafter the “Subject Device.” The Subject Device is currently located at the FBI building, located at 2001 Freedom Way in Roseville, California.

This warrant authorizes the forensic examination of the Subject Device for the purpose of identifying the electronically stored information described in Attachment B.



**ATTACHMENT B**

1. All records on the Subject Device described in Attachment A that relate to violations of 18 U.S.C. § 1591(a)(1) and involve Angel Jesus Sanchez-Manriquez, including:

- a) Records, images, audio, videos, and communications regarding A.G.;
- b) Records, images, audio, videos, and communications regarding the management of prostitution activity;
- c) Records, images, audio, videos, and communications regarding the advertisements of acts of prostitution, including use of Skipthegames.com;
- d) Records, images, audio, videos, and communications regarding hotel reservations;
- e) Records, images, audio recordings, videos, and/or communications regarding the physical location of (and transportation to and from) prostitution encounters, including stored geolocation information;
- f) Records, images, audio, video, and/or communications regarding the proceeds of prostitution activity;
- g) Information related to recruitment of individuals for the purpose of prostitution, including social media accounts that were used to engage in such recruitment;
- h) Records, images, audio, video, and communications regarding condoms, and birth control;
- i) Records, images, audio, video, and communication regarding firearms and/or ammunition;
- j) Records, images, audio, video, and communications regarding Yuba County juvenile detention facilities;
- k) Records, images, audio, video, and communications regarding ownership or control of any device assigned telephone numbers 209-420-2671 and/or 530-638-2760 and/or 916-822-9487;
- l) Records, images, audio, video, and communications regarding ownership or control of email account angelosmithx4@gmail.com and angelms99@live.com.

2. Evidence of user attribution showing who used or owned the Subject Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records evidencing the use of the following Internet Protocol addresses:

- 2601:203:c200:a3e0:751d:7159:ce43:9964;
- 2601:203:c200:a3e0:9065:9eb7:3620:b3b4;
- 2601:203:c200:a3e0:111d:70fc:a0e8:cd19;
- 2601:203:c200:a3e0:fcf3:1e26:cb1f:a702;
- 2601:203:c200:a3e0:2ddf:e21f:1c3e:55dd;

to communicate with SkiptheGames.com, including:

- a) Records of Internet Protocol addresses used;
- b) Records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

5. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.